UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	**STIPULATION OF EXPECTED TESTIMONY**
Manning, Bradley E.	)	
PFC, U.S. Army,	)	
HHC, U.S. Army Garrison,	)	**Mr. Alex Withers**
Joint Base Myer-Henderson Hall	)	
Fort Myer, Virginia 22211	)	**DATED: 7 June 2013**

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Mr. Alex Withers were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows:

1. I currently work as an Investigator in the IT Division of Brookhaven National Laboratory (BNL) in Upton, NY. Specifically, I am part of a Cyber Security Incident Response Team (CSIRT). I have held this position for five years (since September of 2008). Prior to that, I worked as an Advanced Technology Engineer, responsible for helping to maintain the computers that process data for our Relativistic Heavy Ion Collider (RHIC) as well as the ATLAS Computing facility (RACF). BNL has the capacity to process large amounts of data through our super computer systems. Accordingly, in my previous position, I was further responsible for helping to manage the queue of jobs submitted from institutions throughout the world, who seek BNL's assistance in processing large amounts of data. I held that position for four years.

2. I hold a Bachelors and a Masters degree in Computer Science. I also hold three certifications from the computer security professional association Global Information Assurance Certification (GIAC) – one in Forensic Analysis, one in Incident Handling, and one in Intrusion Analysis.

3. I first became involved in this case after I discovered suspicious activity on the desktop work station computer assigned to a BNL employee identified as Mr. Jason Katz. Based on BNL's report to federal law enforcement officials, investigators in the present case against PFC Manning became interested in the contents of the BNL desktop computer assigned to Mr. Katz, which I collected and forensically examined.

4. In my CSIRT position, I monitor information system security for BNL. In early March of 2009, I discovered the BNL desktop machine assigned to Jason Katz had a Firefox extension. An extension is a program that runs within the Firefox internet browser and that enhances the user's abilities. For example, an extension could allow a user to project his/her Internet Protocol (IP) to a different location, and route through a different IP address, so that his/her actions on the web would appear to have originated in that location instead of the user's actual location. In this instance, the extension on Mr. Katz's machine implied that Mr. Katz had bypassed BNL proxy servers designed to monitor BNL computers' internet traffic. I further investigated this activity by reviewing logs created by BNL reporting software. This review revealed that Mr. Katz's BNL desktop machine had a large amount of Secure Shell (SSH) traffic. SSH is a computer protocol, or computer communication language, that facilitates secure or encrypted communications. This information, when taken in conjunction with my review of BNL firewall logs, suggested that Mr. Katz was transferring files between his BNL machine and another

PROSECUTION EXHIBIT 74 for identification
PAGE OFFERED:___ PAGE ADMITTED:___
PAGE 1 OF 3 PAGES

computer outside his home using an SSH, or encrypted, connection. I know the network to which he connected was not his home computer, as the IP address to which this connection was made did not match his home IP address. While I could not tell which types of files were transferred, having previously occupied a duty position responsible for many of the same activities as Mr. Katz was then responsible, I know it is possible for a user in Mr. Katz's position to have hidden files in the BNL system and to have used the BNL computing power to run personal tasks. For example, the BNL super computer power could significantly reduce the amount of time it would take to decrypt an encrypted file without a password. I also know that the BNL desktop CD-RW and USB drives would have been enabled on his work computer. These could have been used to transfer data onto removable media.

5. This, and other suspicious activity, resulted in further investigation. Ultimately, our system detected that Mr. Katz's computer had accessed a website known to contain pirated files. We were able to find this because Mr. Katz upgraded to a web browser that had a bug that allowed me to see what websites Mr. Katz was visiting. Pirated files are illegally obtained files. I cannot recall all of the websites visited by Mr. Katz. The only one that I remember specifically is Pirate Bay, a website that allows for the improper downloading of movies and other entertainment media. As this was against user agreement policy, the BNL system automatically blocked Mr. Katz's desktop computer – essentially removing it from the BNL system. The ensuing investigation included the collection of Mr. Katz's BNL desktop computer for forensic imaging and further investigation. I know this because I was part of the team to report the initial suspicious activity to my supervisor Mr. James Fung. I then met with and accompanied responding law enforcement personnel to Mr. Katz's workstation for the collection of his computer. Mr. Katz was present at the time we obtained the BNL computer. It was a Dell Optiplex 960 computer with a Linux operating system, bar code number 138694. At the time of collection, we checked to make sure the computer did not contain any removable media devices such as a thumb drive. Then, my CSIRT colleagues and I accompanied that computer to the forensic laboratory for forensic imaging by Mr. James McManus. Mr. McManus is an IT Architect at BNL.

6. Following this imaging process, our Cyber Security Team further examined this forensic image. I know our team examined it because I participated in that examination. Our investigation revealed that Mr. Katz had password cracking software on his BNL desktop computer. Additionally, the computer housed at least part of an encrypted .zip file, which, it appeared, Mr. Katz had attempted to break into or decrypt using the brute force attack method. The brute force attack method means using a computer-generated or pre-generated list of possible passwords to crack an unknown password by running different passwords against the file one at a time at a very fast rate. We did not have the password to this file and so could not open it. Our search also revealed movies that had been downloaded and saved to Mr. Katz's work computer. I do not recall whether WikiLeaks was mentioned in any way on Mr. Katz's computer. This was prior to my having heard of WikiLeaks, so I may not have noted its significance at the time.

7. At no time, prior to, during, or after the collection of Mr. Katz's BNL computer did I alter its hard drive, its other components, or its contents in any way. Furthermore, I never altered any forensic image made from this computer in any way. At no point did I observe anyone alter the

computer, its hard drive, its other components, or its contents in any way. Likewise, I have no reason to believe the evidence was damaged or contaminated in any way.

ASHDEN FEIN	THOMAS F. HURLEY	BRADLEY E. MANNING
MAJ, JA	MAJ, JA	PFC, USA
Trial Counsel	Defense Counsel	Accused